PCT / IB 00 / 00847
30. 06. 00

IB 00/00947

SCHWEIZERISCHE EIDGENOSSENSCHAFT
CONFÉDÉRATION SUISSE
CONFEDERAZIONE SVIZZERA

REC'D 07 JUL 2000
WIPO PCT

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

4

Bescheinigung

Die beiliegenden Akten stimmen mit den ursprünglichen technischen Unterlagen des auf der nächsten Seite bezeichneten Patentgesuches für die Schweiz und Liechtenstein überein. Die Schweiz und das Fürstentum Liechtenstein bilden ein einheitliches Schutzgebiet. Der Schutz kann deshalb nur für beide Länder gemeinsam beantragt werden.

Attestation

Les documents ci-joints sont conformes aux pièces techniques originales de la demande de brevet pour la Suisse et le Liechtenstein spécifiée à la page suivante. La Suisse et la Principauté de Liechtenstein constituent un territoire unitaire de protection. La protection ne peut donc être revendiquée que pour l'ensemble des deux Etats.

Attestazione

Gli uniti documenti sono conformi agli atti tecnici originali della domanda di brevetto per la Svizzera e il Liechtenstein specificata nella pagina seguente. La Svizzera e il Principato di Liechtenstein formano un unico territtorio di protezione. La protezione può dunque essere rivendicata solamente per l'insieme dei due Stati.

Bern, 26. Juni 2000

Eidgenössisches Institut für Geistiges Eigentum
Institut Fédéral de la Propriété Intellectuelle
Istituto Federale della Proprietà Intellettuale

Patentverfahren
Administration des brevets
Amministrazione die brevetti

Rolf Hofstetter


de la Propriété Intellectu

Demande de brevet no 1999 1438/99

CERTIFICAT DE DEPOT (art. 46 al. 5 OBI)

L'Institut Fédéral de la Propriété Intellectuelle accuse réception de la demande de brevet Suisse dont le détail figure ci-dessous.

Titre:
Méthode et dispositif pour garantir l'intégrité et l'authenticité d'un ensemble de données.

Requérant:
Nagravision S.A.
22, Route de Genève
1033 Cheseaux-sur-Lausanne

Mandataire:
Griffes Consulting S.A.
Rte de Florissant, 81
CH-1206 GENEVE

Date du dépôt: 04.08.1999

Classement provisoire: G06K

METHODE ET DISPOSITIF POUR GARANTIR L'INTEGRITE ET L'AUTHENTICITE D'UN ENSEMBLE DE DONNEES

La présente invention est relative au domaine du contrôle d'intégrité et d'authenticité de données, en particulier lors du téléchargement de logiciels.

L'invention s'applique à toute machine comprenant au moins une unité centrale telle que couramment connue et utilisée en informatique, au sens d'un processeur possédant au moins une partie de son programme dans une mémoire à écriture multiple.

Il est connu qu'une altération ou corruption de données laisse des traces dans certaines parties des informations traitées et stockées dans une mémoire, avant ou après traitement. Il est connu d'utiliser une technique mathématique simple telle que le calcul du "checksum" afin de déterminer si les données prises en considération ont été modifiées depuis l'établissement du checksum de référence.

Néanmoins, la plupart des systèmes checksum ont des faiblesses. Ainsi, il peut y avoir, au cours des opérations mathématiques, propagation d'erreurs aléatoires qui peuvent se compenser, donnant un résultat identique à celui attendu. En conséquence, la vérification par les méthodes connues sera inopérante dans certains cas.

Il y a donc un défi non résolu de façon satisfaisante à ce jour, qui consiste à améliorer la fiabilité et la sécurité procurée par les opérations dites de checksum, en particulier dans les données transmises par voies publiques et destinées à être stockées dans une mémoire programme.

Le but visé par la présente invention est atteint par le fait que l'on adjoint aux données à transmettre un bloc de contrôle comprenant le résultat d'une opération effectuée sur tout ou partie desdites données, opération de type unidirectionnelle et sans collision.

Dans le cadre de l'invention, un message est un ensemble de données destiné à la mise à jour ou le chargement d'un logiciel.

On entend par opération unidirectionelle une opération qu'il est aisé de réaliser dans un sens mais quasiment impossible dans l'autre. Pour exemple, l'opération x^y est facile à réaliser mais l'opération $\sqrt[y]{x}$ est bien plus difficile.

On entend par opération sans collision une opération pour laquelle aucune combinaison différente des données en entrée ne donne un résultat similaire.

Dans le cadre de l'invention, cette opération unidirectionelle est une application mathématique H d'un ensemble source vers un ensemble objet, dans laquelle chaque élément x de l'ensemble source se voit attribuer une image H(x). Ces fonctions sont particulièrement utiles lorsque ce sont des fonctions dites Hash, telles que définies en page 27 de l'ouvrage RSA Laboratories' Frequently Asked Questions About Today's Cryptography, v4.0. L'élément x peut être d'une longueur quelconque mais H(x) est toujours une suite de caractères de longueur fixe ("fixed-size string"). Une telle fonction est difficile à inverser, c'est-à-dire que la connaissance de H(x) ne permet en général pas de retrouver x. Elle est de plus dite libre de collision lorsqu'elle est injective, c'est-à-dire que $H(y)=H(x)$ entraîne nécessairement $y=x$, de même que $H(y)\neq H(x)$ entraîne nécessairement $y\neq x$.

L'invention consiste à remplacer les opérations connues de checksum par l'utilisation de fonctions unidirectionnelles, et particulièrement de fonctions Hash.

Dans une forme particulière de réalisation, l'ensemble considéré comprend une partie émission, située dans une station de gestion, et une partie réception qui peut être constituée par un nombre relativement grand d'unités périphériques fonctionnellement semblables. Le but est de garantir que le logiciel envoyé par la partie émission est reçu de manière authentique et intégrale par chacune des unités périphériques. Par analogie avec le vocabulaire de la télévision à péage, qui constitue une application importante mais non exclusive de l'invention, ces

unités périphériques seront dans la suite de l'exposé appelées IRD soit Integrated Receiver Decoder comprenant une partie récepteur, un décodeur pour le traitement du signal reçu par le décodeur, un processeur central ou CPU qui travaille de préférence avec une mémoire non volatile ainsi que divers périphériques.

Une mémoire non volatile est une mémoire dont le contenu est maintenu même lors de la coupure de l'alimentation principale, par exemple au moyen d'une source d'énergie autonome telle que batterie ou pile. D'autres types de mémoires non volatiles peuvent être utilisées, telles que des mémoires dites EEPROM, Flash EPROM ou encore FEPROM. C'est cette mémoire non volatile qui contient les données sauvegardées en cas d'interruption de l'alimentation électrique. Elle est essentielle pour le bon fonctionnement du processeur de l'IRD.

Les informations sont reçues par l'IRD en provenance de la station de gestion, sous forme d'un flux de données arrivant au récepteur de l'unité IRD. Dans le cas de la télévision codée, ou plus généralement interactive, le flux de données comprend des informations vidéo, des informations audio, des informations de données, des applications exécutables telles que des "applets", et enfin des informations de contrôle de données de divers types.

Il s'agit dans ce cas de s'assurer que ces informations sont correctement reçues et interprétées par l'IRD avant leur stockage en mémoire opérationnelle, en particulier les données qui seront exécutées c'est-à-dire le logiciel.

Le récepteur de l'IRD les transmet à un décodeur, qui lui-même les met en circulation dans l'IRD au moyen d'un bus. Sur ce bus sont connectés un processeur spécialisé dans le multimédia, lui-même connecté à un écran de visualisation ainsi qu'à un ou plusieurs haut-parleurs, la mémoire non volatile précitée, et un ou plusieurs sous-ensembles optionnels. C'est le processeur de l'IRD (CPU) qui administre et contrôle le fonctionnement de celui-ci, ainsi que les différents sous-ensembles tels qu'un canal de test, une interface pour carte à puce, une mémoire auxiliaire dite de masse, d'autres processeurs, ou encore un

modem. De plus, la station de gestion peut recevoir des informations en retour, par exemple par le biais du modem connecté au réseau public de télécommunications.

Ces sous-ensembles peuvent eux-mêmes être la source d'erreurs qu'il s'agit de détecter et de corriger, notamment dans le cas du chargement d'une nouvelle version du logiciel de fonctionnement de l'IRD et particulièrement de son CPU, ou de certains programmes exécutables par l'IRD ou ses composants.

Le logiciel et les données dont l'authenticité et l'intégrité doivent être garanties peuvent être chargés par divers moyens. L'un de ces moyens consiste, comme il a été dit, à utiliser le récepteur précité, en envoyant vers ce récepteur avec le flux de données, et en l'identifiant de manière reconnaissable par l'unité centrale, une mise à jour de mémoire comprenant plusieurs blocs de données M1; M2, ...Mn ainsi qu'une en-tête permettant d'identifier les données M1 à Mn.

Alternativement ou en complément, les blocs de données et l'en-tête peuvent parvenir à l'IRD par l'un de ses sous-ensembles optionnels tel le modem par exemple.

Les blocs de données M1, M2, ...Mn peuvent sans inconvénient être envoyés en clair, c'est-à-dire sans encryptage à ce stade, dans le cadre de l'invention.

La méthode selon l'invention consiste, dans cette forme, à appliquer d'abord, au stade de l'émission, une fonction unidirectionnelle ou fonction "hash" à tout ou partie des blocs de données M1, M2, ...Mn pour obtenir un résultat Hx représentatif de l'ensemble M1 à Mn. On peut également traiter les blocs de données M1 à Mn séparément et obtenir le résultat Hx1 correspondant à M1, Hx2 correspondant à M2 ... et Hxn correspondant à Mn. Ce ou ces résultats Hx sont placés dans un bloc de contrôle qui peut être une partie de l'en-tête à un emplacement non aléatoire. Lorsque plusieurs résultats Hx sont générés, représentatifs de chaque partie Mn, ils sont placés à divers emplacements répartis dans le bloc de contrôle. Le bloc de contrôle comprend également des

informations de service IS telles que la version des données Mn, la date de mise en service ou la durée de validité de ces données.

Un domaine particulièrement crucial pour l'authentification des données concerne les systèmes pour lesquels les données sont transmises par des voies publiques tels que voie hertzienne, téléphonique ou Internet. Dans ce cas, un intrus peut se substituer à une station de gestion et envoyer des données pour modifier le fonctionnement du système cible.

La présente invention s'étend également à une méthode pour garantir l'authenticité de l'émetteur du message en transmettant tout ou partie du bloc de contrôle sous forme d'un cryptogramme. Dans une forme d'exécution, ce cryptogramme est calculé sur l'ensemble des données du bloc de contrôle. Le message se compose d'une partie identification en clair pour annoncer le type de message arrivant à l'unité périphérique, d'une signature représentant le bloc de contrôle crypté et des données M1 à Mn. De la même manière que pour le calcul de la fonction Hx, cette signature peut se décomposer en plusieurs signatures (Sx1, Sx2 ... Sxn) sur des parties du bloc de contrôle différents. Par exemple, les informations relatives aux données M1, soit le résultat Hx1 ainsi que les données de services associées IS1, sont cryptées pour former le cryptogramme Sx1. Cet algorithme d'encryptage peut, de manière connue, comprendre l'utilisation d'une clé asymétrique sous forme privée, c'est-à-dire utiliser la clé privée de l'algorithme RSA.

Il ne reste plus que d'assembler le bloc identificateur, le bloc de contrôle sous sa forme en clair (sans fonction de cryptage) ou sous sa forme cryptée, aux données proprement dites M1, M2...Mn, et d'envoyer ce message vers le ou les IRD.

La partie réception de l'IRD effectue le stockage temporaire du message et, si le bloc de contrôle est crypté, l'IRD détermine le bloc de contrôle en clair par l'application au bloc crypté de l'algorithme de décryptage en utilisant la clé publique de l'algorithme RSA.

Un fois que le bloc de contrôle est disponible en clair, l'IRD applique la même fonction unidirectionnelle que lors de l'émission sur les blocs de données M1 à Mn pour déterminer le ou les résultats Hy de la fonction hash, résultats qui seront comparés aux données contenues dans le bloc de contrôle.

Si la comparaison Hx=Hy est positive, on peut affirmer que les données M1 à Mn n'ont pas été corrompues ou modifiées lors du transport, et, si l'opération de cryptage du bloc de contrôle a été appliquée, on peut de plus affirmer que les données sont bien de l'auteur duquel ces données sont attendues.

Dans ce cas, l'opération est considérée comme réussie et les nouvelles données peuvent, soit immédiatement, soit à une date convenue, être transférées de la mémoire temporaire (M1 à Mn) à la mémoire opérationnelle (M1' à Mn').

Dans une forme particulière de réalisation de l'invention, le bloc de contrôle comprend également un ou des certificats délivrés par une autorité extérieure à la station de gestion. Par analogie aux résultats de la fonctions hash sur les données, le certificat Cx peut se décomposer en un certificat Cx1 correspondant à M1, Cx2 correspondant à M2 ... et Cxn correspondant à Mn. On dénommera Cx l'ensemble de ces certificats pour la suite de la description. Des exemples de méthodes de détermination d'un certificat d'authenticité sont décrites dans le documents US 5'373'561, US 5'136'646 et US 5'136'647.

Dans une forme particulière de réalisation de l'invention, ces certificats comprennent une information d'un horodateur digital ou encore "Timestamp". Ce certificat présente l'avantage de représenter indiscutablement l'ensemble des données M1 à Mn car ces données ont été présentées à une autorité externe qui a livré en retour des informations dites d'authentification permettant de retracer l'origine des données. Ceci présente l'avantage de permettre de situer l'origine d'une erreur d'une façon indiscutable, car prouvée par une autorité reconnue, ainsi que, du point de vue du droit, de prouver la non-implication de telle ou telle partie de la procédure dans l'erreur détectée. Ceci est important lorsque l'erreur peut avoir des conséquences juridiques.

La force de la méthode réside en partie dans la qualité de la fonction unidirectionnelle H et dans la signature cryptographique de celle-ci. Ainsi, un simple checksum ne permet pas de détecter l'échange de deux blocs de caractères dans les données puisque l'addition est réputée, en mathématiques, commutative et associative. Par contre, un résultat de fonction "hash" Hx est une image très réaliste de x, même si x est beaucoup plus long que Hx. Si des échanges de caractères sont effectués dans la suite de caractères x, la fonction H(x) le détectera immédiatement, et le système ne pourra pas fonctionner suite à cette détection. Il en résulte une sécurité accrue.

Un aspect important de l'invention est de permettre de vérifier à tous moments la validité des données en mémoire dans l'unité périphérique. En effet, la présence en mémoire de ces informations de contrôle permet à l'unité de procéder à une auto-vérification fiable. Cette vérification donne un résultat sans comparaison avec le checksum habituellement appliqué sur la mémoire programme. Si cette vérification donne un résultat différent que celui de référence, l'unité dispose de moyens (liaison modem, liaison sur canal câblé) pour informer une entité extérieure, par exemple la station de gestion, de la non conformité du programme.

Si le moyen préférentiel de l'invention pour la génération et la transmission des informations de contrôle est la station de gestion, l'invention recouvre une unité périphérique dont tout ou partie du programme est initialement chargé avec les informations de contrôle tels que décrit ci-dessus. Ceci peut être effectué dans un site de fabrication ou lors de l'initialisation précédant la vente au moyen du processeur, ou par téléchargement de ces informations de contrôle par l'un des périphériques à une étape d'initialisation.

La présente invention sera comprise plus en détail grâce aux dessins suivants, pris à titre non limitatifs, dans lesquels:

- la figure 1 représente le mécanisme de préparation du message d'envoi de données; et

- la figure 2 représente un schéma bloc d'un IRD.

Sur la figure 1, les données composant un logiciel sont divisées en blocs de données M1 à Mn. Ces données sont traitées par la fonction hash afin de déterminer les résultats Hx1 à Hxn représentatifs de l'ensemble des données. Sur ce diagramme, la partie optionnelle qui consiste à joindre aux résultats Hx des certificats Cx1 à Cxn est représentée par le bloc AE qui signifie autorité externe. Cette autorité externe retourne les certificats Cx. Le bloc de contrôle CB est alors composé des résultas Hx et des certificats Cx. Des informations de service IS caractérisant les données sont également jointes.

Dans la forme d'exécution incluant le cryptogramme Sx, le bloc de contrôle (CB) précédemment composé est traité pour cryptage par la clé privée PrK de la station de gestion.

Le résultat final, tel qu'illustré sur la figure 1, représente le message prêt à l'envoi et débuté par l'identificateur de message Id, le bloc de contrôle crypté Sx et les données M1 à Mn.

Sur la figure 2, un IRD ou Integrated Receiver Decoder est représenté, constituant la partie périphérique de l'ensemble auquel est appliquée la méthode selon l'invention dans le mode de réalisation décrit ci-après. Cette IRD comprend un bus central DB sur lequel viennent se connecter tous les différents modules. Le module central de l'IRD est constitué par le processeur CPU qui a pour tâche d'effectuer les différents traitements.

Un récepteur REC reçoit un flux de données comprenant des informations vidéo, audio, des données et des applications exécutables via des supports aussi variés que le câble, une antenne hertzienne, une parabole satellite, Internet ou autres technologies connues. Ce récepteur REC est relié à une interface DC, elle-même connectée au bus DB.

Sur ce bus DB sont aussi connectés:

- un processeur multimédia MP spécialisé dans le traitement des informations vidéo ou audio, qu'il dirige respectivement vers un écran de visualisation VD et des haut-parleurs AD;

- un canal de test TC, lui-même pouvant être relié à un testeur TEST servant aux réglages d'usine et à la maintenance;

- une mémoire non volatile NVM, rendue indépendante de l'alimentation principale par sa propre source d'alimentation;

- une interface INT pour carte à puce, recevant physiquement une carte à puce SM;

- une mémoire auxiliaire ou encore mémoire de masse TMEM;

- un modem MD, connecté au réseau public NET, celui-ci adoptant des technologies et supports connus;

- d'autres processeurs OP, DP assumant diverses fonctions au gré de l'utilisateur, notamment celles de traitement de données Data.

C'est le CPU qui contrôle les mises à jour de logiciel dont un exemple va être décrit. Il les accepte ou les rejette en fonction du résultat des tests réalisés selon la méthode qui fait l'objet de l'invention.

Ces versions de logiciel du CPU de l'IRD peuvent parvenir à l'IRD par le récepteur REC, par le testeur TEST, par la carte à puce SM, ou encore par le réseau NET. Dans la suite, on décrira plus avant le cas où elles arrivent à l'IRD par le récepteur REC avec le flux d'informations vidéo et audio.

Un ensemble de données, représentant une nouvelle version de logiciel arrivant à l'IRD, est stocké en mémoire de l'IRD, avec les informations de service, après avoir été contrôlé quant à son authenticité et son intégrité. Ceci permet à la station de gestion de charger cette version de logiciel dans un grand nombre

d'IRD périphériques, et de déclencher sa mise en service sans erreur par l'ensemble de ces IRD.

L'invention ne se limite pas aux exemples cités plus haut et s'étend à d'autres formes de réalisation. Par exemple, il est possible de transmettre dans le bloc de contrôle les résultats Hx et les cryptogrammes Sx. De ce fait, les opérations de vérification d'intégrité peuvent se faire indépendamment des opérations de vérification d'authenticité. L'ordre des informations tel que décrit sur la figure 1 est indiqué à titre d'exemple non limitatif et peut être quelconque.

Il est à noter que les informations de vérification du bloc de contrôle CB telles que le code Hx et la signature Sx, sont mémorisées dans l'IRD pour utilisation future. C'est ainsi qu'une validation ou confirmation de l'intégrité et l'authenticité du logiciel peut à tout moment être demandée à l'IRD, par la carte à puce SM, le testeur TEST, ou sur requête arrivant par le réseau NET ou le récepteur REC. Dans ce cas, l'IRD recalculera ces différents paramètres Hy et comparera ces dernières avec les valeurs mémorisées de référence. De même, le CPU peut lui aussi, à intervalles réguliers, déclencher cette procédure de vérification.

Dans une autre forme d'exécution, la vérification est effectuée, non pas par le CPU, mais par une entité extérieure tel que le testeur TEST, ou via le réseau NET ou la liaison REC. Dans ce cas, tout ou partie des données Mn sont transmises pour vérifications des informations de contrôle Hy, informations qui sont comparées avec les valeurs Hx d'origine. Une vérification supplémentaire peut être faite avec les valeur Hx mémorisées par l'IRD.

Selon une forme d'exécution de l'invention, les informations de vérification (Hx, Sx) sont mémorisées dans l'un des périphériques, par exemple la carte à puce SM qui est réputée inviolable. De ce fait, il n'est pas possible de modifier Hx pour qu'il corresponde avec Hy, quant bien même les données M1 à Mn sont différentes.

Pour la fonction de cryptage, il est recommandé d'utiliser un algorithme A faisant appel à une clé asymétrique sous forme privée PrK. C'est par exemple le cas des algorithmes de type RSA (Rivest, Shamir & Adleman). Cet algorithme est appliqué sur le bloc de contrôle uniquement pour des raisons pratiques. On pourrait l'appliquer également sur l'ensemble des données selon le temps disponible pour cette opération ou la longueur des données.

Un fois le message reçu par l'IRD, le message est décomposé et les différents éléments stockés dans la mémoire temporaire TMEM. L'IRD applique aux blocs de données M1 à Mn le même traitement que lors de l'émission mais dans l'ordre inverse. Il est clair que dans le cas où l'on reçoit le bloc de contrôle sous forme chiffrée, la première opération consiste à décrypter le bloc de contrôle par la clé publique PuK pour obtenir le bloc de contrôle en clair CB'.

L'étape suivante consiste à effectuer la fonction unidirectionnelle H sur les données M1 à Mn avec pour résultats les valeurs Hy1 à Hyn. Dans le cas où une erreur s'est glissée dans les blocs mémoire M1, M2, ...Mn pendant la transmission du message, cette erreur se répercute sur Hy qui se trouve alors être différent de Hx contenu dans le bloc de contrôle et les données M1 à Mn seront rejetées. Ainsi, l'obtention des valeurs de référence Hx par une fonction cryptographique, ajouté au calcul de la fonction H sur les données, permet de garantir l'intégrité et l'authenticité des données M1 à Mn.

Comme exemple de fonctions H, on connaît les fonctions MD2, MD5 et SHA-1.

Revendications

1. Méthode pour contrôler l'intégrité et l'authenticité d'un message contenant du logiciel généré par une station émettrice et transmis à une ou plusieurs unités réceptrices (IRD), message comprenant une partie identification (Id), une partie données (M1 à Mn) et au moins un bloc de contrôle (CB) comprenant des informations de service (IS), caractérisée en ce que cette méthode consiste à générer et inclure au bloc de contrôle (CB) une information de contrôle (Hx) représentative du résultat d'une fonction dite unidirectionnelle et sans collision, effectuée sur tout ou partie des données (M1 à Mn).

2. Méthode selon la revendication 1, caractérisée en ce que la fonction unidirectionnelle et sans collision est de type MD2 , MD5 ou SHA-1.

3. Méthode selon les revendications 1 ou 2, caractérisée en ce qu'elle consiste à joindre au bloc de contrôle (CB) un certificat (Cx) représentant un cryptogramme sur tout ou partie des données, délivré par une autorité extérieure habilitée à certifier des données.

4. Méthode selon l'une des revendications précédentes, caractérisée en ce qu'elle consiste à transmettre le bloc de contrôle (CB) sous forme d'une signature (Sx) représentant un cryptogramme résultant d'une opération de cryptage sur tout ou partie dudit bloc de contrôle.

5. Méthode selon les revendications 1, 2 ou 3, caractérisée en ce qu'elle consiste à joindre au bloc de contrôle (CB) une signature (Sx) représentant un cryptogramme résultant d'une opération de cryptage sur tout ou partie dudit bloc de contrôle.

6. Méthode selon les revendications 4 et 5, caractérisée en ce que cette opération de cryptage est de type RSA basée sur une clé dite privée (PrK).

7. Méthode selon les revendications 1, 2, 3 ou 5, caractérisée en ce qu'elle consiste, à la réception, à mémoriser les informations (Hx) du bloc de contrôle,

de calculer les valeurs (Hy) représentative du résultat d'une fonction dite unidirectionnelle et sans collision effectuée sur tout ou partie des données (M1 à Mn), vérifier les valeurs calculées (Hy) avec celles reçues (Hx) et rejeter les données (M1 à Mn) si les deux valeurs diffèrent.

8. Méthode selon les revendications 4 ou 5, caractérisée en ce qu'elle consiste, à la réception, à mémoriser les informations (IS, Hx, Sx) du bloc de contrôle (CB), de déchiffrer le bloc de contrôle (CB') contenant les valeurs (Hx) par un algorithme de décryptage, à calculer les valeurs (Hy) représentative du résultat d'une fonction dite unidirectionnelle et sans collision effectuée sur tout ou partie des données (M1 à Mn), à comparer les valeurs calculées (Hy) avec celles contenue dans le bloc de contrôle déchiffré (Hx) et rejeter les données (M1 à Mn) si les deux valeurs diffèrent.

9. Méthode selon la revendication 8, caractérisée en ce que cette opération de décryptage est de type RSA basée sur une clé dite publique (PuK).

10. Méthode selon la revendication 9, caractérisée en ce que la clé publique (PuK) servant à déchiffrer le bloc de contrôle (CB') est stockée hors de l'unité réceptrice (IRD).

11. Méthode selon l'une des revendications précédentes, caractérisée en ce que l'unité réceptrice (IRD) peut calculer périodiquement ou sur requête les valeurs (Hy) représentative du résultat d'une fonction dite unidirectionnelle et sans collision effectuée sur tout ou partie des données (M1 à Mn) en mémoire opérationnelle (NVR), vérifier les valeurs calculées (Hy) avec celles mémorisées de référence (Hx) et rejeter les données (M1 à Mn) si les deux valeurs diffèrent.

12. Méthode selon la revendication 11, caractérisée en ce que la vérification des données (M1 à Mn) peut être effectuée à l'extérieur de l'unité réceptrice (IRD) en transmettant tout ou partie des données (M1 à Mn) à une unité de contrôle (TEST, SM, NET).

13. Unité réceptrice (IRD) de message de logiciel comprenant un processeur (CPU), une mémoire opérationnelle (NVM) contenant des données (M1' à Mn') représentant du logiciel, et des informations de contrôle (Hx), caractérisée en ce qu'elle comprend des moyens pour calculer une fonction (Hy) dite unidirectionnelle et sans collision sur tout ou partie des données (M1' à Mn'), des moyens pour comparer le résultat (Hy) avec les informations de contrôle (Hx) ainsi que des moyens pour informer une entité extérieure si les deux valeurs Hx et Hy diffèrent.

14. Unité réceptrice selon la revendication 13, caractérisée en ce qu'elle comprend une mémoire temporaire (TMEM), des moyens pour détecter un message de données (M1 à Mn) représentant un logiciel et comprenant un bloc de contrôle (CB), des moyens pour stocker ledit message de logiciel dans la mémoire temporaire (TMEM), des moyens pour calculer une fonction cryptographique asymétrique permettant de retrouver les informations de contrôle (Hx) contenue dans le bloc de contrôle (CB), des moyens pour calculer une fonction (Hy) dite unidirectionnelle et sans collision sur tout ou partie des données (M1 à Mn), des moyens pour comparer le résultat (Hy) avec l'information de contrôle (Hx) contenue dans le message reçu et des moyens pour transférer les données (M1 à Mn) de la mémoire temporaire (TMEM) à la mémoire opérationnelle (NVM) dans le cas où le résultat de la comparaison est positif.

ABREGE

Afin de garantir l'intégrité et l'authenticité des données transmises entre une station de gestion et une ou plusieurs unités réceptrices, la méthode consiste à joindre au message transmis, un bloc de contrôle comprenant le résultat d'une fonction unidirectionnelle et sans collision effectuée sur tout ou partie des données à transmettre.

(Figure 1)

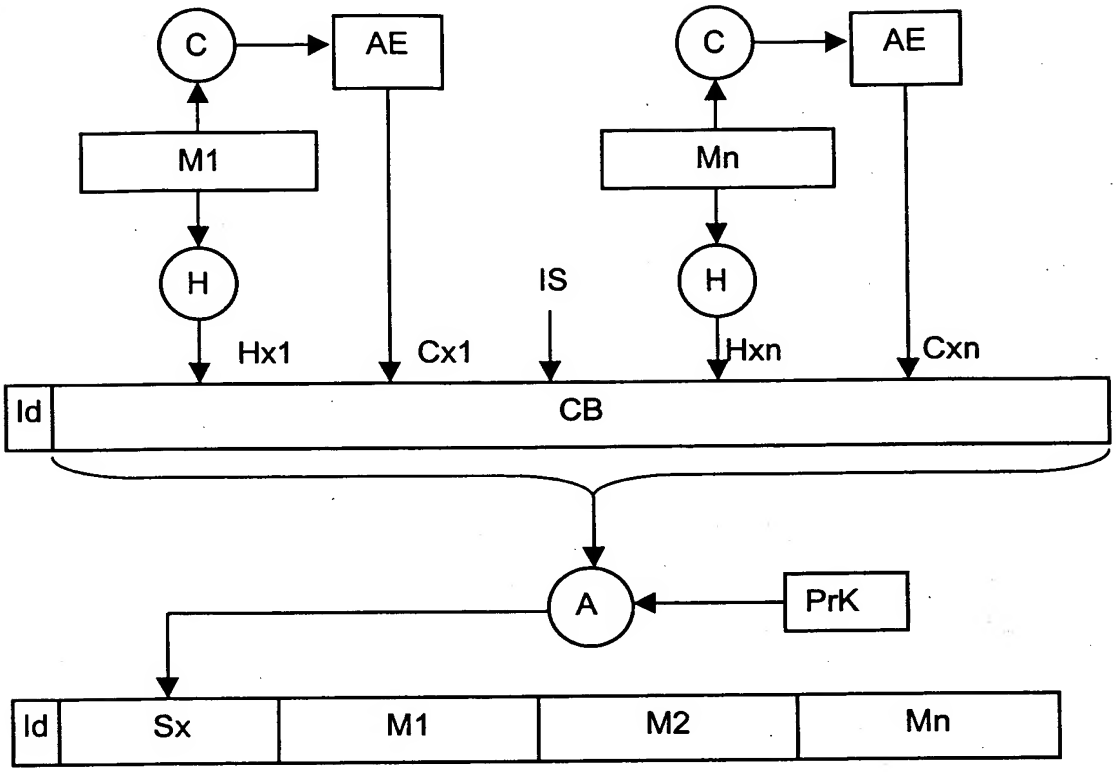

Fig. 1

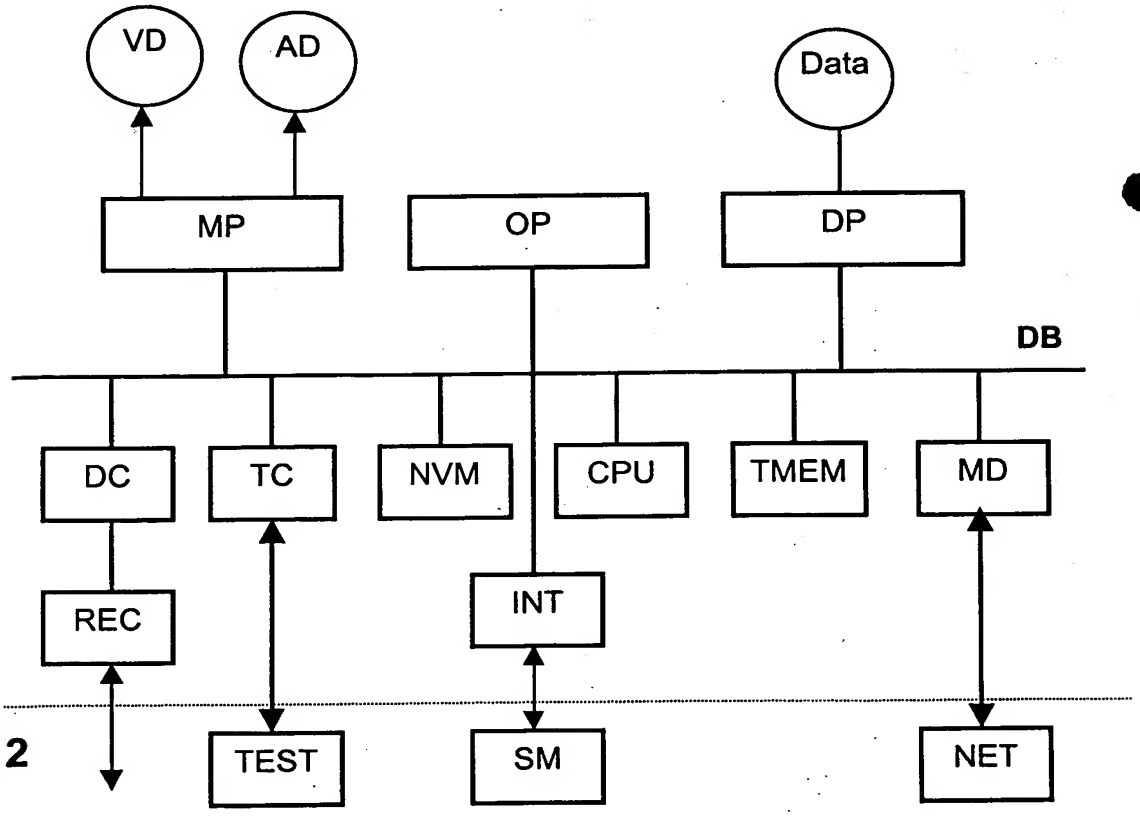

Fig. 2